PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2001-312402
(43)Date of publication of application : 09.11.2001

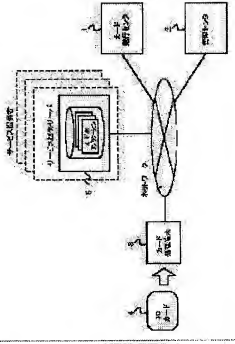
(51)Int.Cl. G06F 9/06
G06F 9/445
G06K 17/00
G06K 19/07
G06K 19/00

(21)Application number : 2000-129056
(22)Date of filing : 28.04.2000

(71)Applicant : NTT DATA CORP
(72)Inventor : YAMAZAKI KENJI
SAKAI TAKAAKI
AMAMIYA SHUNICHI
TAMAI JUN
TOMINAGA HIROSHI
TAKAGI SOICHIRO

(54) CARD SYSTEM, IC CARD, AND RECORDING MEDIUM

(57)Abstract:
PROBLEM TO BE SOLVED: To provide a card system, etc., which can safely supply an application.
SOLUTION: An IC card 4 stores a permission table where the hash value of an application allowed by a card issue center 1 to be supplied is set. The IC card 4 obtains the hash value of an application supplied from a service providing server 5, decides whether the hash value matches the hash value registered in the permission table, and stores the application in a prescribed area of the IC card 4 when they match each other, but performs prescribed error processing when not.



LEGAL STATUS

[Date of request for examination] 04.04.2005
[Date of sending the examiner's decision of rejection]
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]
[Date of final disposal for application]
[Patent number]
[Date of registration]

[Number of appeal against examiner's decision of rejection]
[Date of requesting appeal against examiner's decision of rejection]
[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)**公開特許公報**（Ａ）　(11)特許出願公開番号
特開2001－312402
（P2001－312402A）
(43)公開日　平成13年11月９日(2001.11.9)

(51)Int.Cl.[7]	識別記号	ＦＩ		テーマコード（参考）
Ｇ０６Ｆ　9/06	５５０	Ｇ０６Ｆ　9/06	５５０Ｇ	５Ｂ０３５
9/445		Ｇ０６Ｋ　17/00	Ｂ	５Ｂ０５８
Ｇ０６Ｋ　17/00			Ｄ	５Ｂ０７６
		Ｇ０６Ｆ　9/06	４２０Ｊ	
19/07		Ｇ０６Ｋ　19/00	Ｎ	

審査請求　未請求　請求項の数12　ＯＬ　（全 14 頁）　最終頁に続く

(21)出願番号　特願2000－129056(P2000－129056)

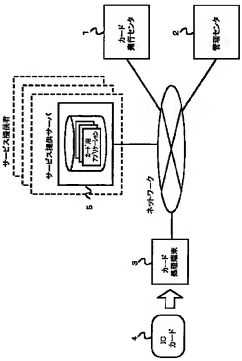
(22)出願日　平成12年４月28日(2000.4.28)

(71)出願人　000102728
株式会社エヌ・ティ・ティ・データ
東京都江東区豊洲三丁目３番３号
(72)発明者　山崎　研史
東京都江東区豊洲三丁目３番３号　株式会社エヌ・ティ・ティ・データ内
(72)発明者　酒井　敏明
東京都江東区豊洲三丁目３番３号　株式会社エヌ・ティ・ティ・データ内
(74)代理人　100095407
弁理士　木村　満

最終頁に続く

(54)【発明の名称】　カードシステム、ＩＣカード及び記録媒体

(57)【要約】
【課題】　アプリケーションの供給を安全に行うことができるカードシステム等を提供する。
【解決手段】　ＩＣカード４は、カード発行センタ１により供給が許可されたアプリケーションのハッシュ値が設定されている許可テーブルを記憶する。ＩＣカード４は、サービス提供サーバ５から供給されたアプリケーションについてハッシュ値を求め、許可テーブルに登録されているハッシュ値と合致するか否かを判別し、合致する場合、そのアプリケーションをＩＣカード４の所定領域に記憶し、合致しない場合、所定のエラー処理を行う。



1

【特許請求の範囲】

【請求項１】カード発行センタにより発行されたＩＣカードに、供給センタにより供給されるアプリケーションを記憶するカードシステムであって、

前記ＩＣカードは、

前記カード発行センタにより供給が許可されたアプリケーションに関する許可テーブルを記憶し、

前記供給センタから供給されたアプリケーションが前記許可テーブルに登録されているか否かを判別し、

前記アプリケーションが前記許可テーブルに登録されている場合、該アプリケーションを当該ＩＣカードの所定領域に記憶し、

前記アプリケーションが前記許可テーブルに登録されていない場合、所定のエラー処理を行う、

ことを特徴とするカードシステム。

【請求項２】前記許可テーブルには、各前記アプリケーションについて、当該アプリケーション基づいて導出されるチェック情報がそれぞれ設定され、

前記ＩＣカードは、

前記供給センタからのアプリケーションの供給に応答し、前記供給されたアプリケーションに基づいてチェック情報を導出し、前記許可テーブルに設定されている該当するアプリケーションのチェック情報と照合し、

前記チェック情報が合致する場合には、前記供給されたアプリケーションを当該ＩＣカードの所定領域に記憶し、

前記チェック情報が合致しない場合には、所定のエラー処理を行う、

ことを特徴とする請求項１に記載のカードシステム。

【請求項３】前記チェック情報はハッシュ値を含む、

ことを特徴とする請求項２に記載のカードシステム。

【請求項４】前記許可テーブルには、管理機関による署名が付与されている、

ことを特徴とする請求項１又は２に記載のカードシステム。

【請求項５】カード発行センタにより発行されたＩＣカードに、供給センタにより供給されるアプリケーションを記憶するカードシステム用のＩＣカードであって、

前記カード発行センタにより供給が許可されたアプリケーションに関する許可テーブルを記憶し、

前記供給センタから供給されたアプリケーションが前記許可テーブルに登録されているか否かを判別し、

前記アプリケーションが前記許可テーブルに登録されている場合、該アプリケーションを当該ＩＣカードの所定領域に記憶し、

前記アプリケーションが前記許可テーブルに登録されていない場合、所定のエラー処理を行う、

ことを特徴とするＩＣカード。

【請求項６】カード発行センタにより発行されたＩＣカードに、供給センタにより供給されるアプリケーション

2

を記憶するカードシステムであって、

前記供給センタは、前記カード発行センタから認証情報を取得し、取得した前記認証情報とアプリケーションを前記ＩＣカードに供給し、

前記ＩＣカードは、前記供給センタからの前記認証情報の正当性をチェックし、チェック結果が正常を示す場合、前記供給センタからのアプリケーションを当該ＩＣカードの所定領域に記憶し、チェック結果がエラーを示す場合、所定のエラー処理を行う、

ことを特徴とするカードシステム。

【請求項７】前記供給センタは、ＩＣカードにアプリケーションを供給するとき、アプリケーションの供給先のＩＣカードからカード識別符号を取得し、取得した前記カード識別符号とアプリケーション識別符号を前記カード発行センタに供給し、

前記カード発行センタは、前記アプリケーション識別符号に基づくアプリケーションに関する情報を、前記カード識別符号により特定されるＩＣカードの鍵で暗号化したものを前記認証情報として前記供給センタに供給し、

前記ＩＣカードは、当該ＩＣカードの鍵を用いて前記認証情報の正当性をチェックする、

ことを特徴とする請求項６に記載のカードシステム。

【請求項８】供給センタは、ＩＣカードにアプリケーションを供給するとき、アプリケーションの供給先のＩＣカードから乱数を取得し、取得した乱数とアプリケーション識別符号を前記カード発行センタに供給し、

前記カード発行センタは、前記乱数と前記アプリケーション識別符号に基づくアプリケーションに関する情報を当該カード発行センタの鍵で暗号化したものを前記認証情報として前記供給センタに供給し、

前記ＩＣカードは、乱数を生成して前記供給センタに供給し、前記供給センタから供給された前記認証情報の正当性を前記カード発行センタの鍵を用いてチェックする、

ことを特徴とする請求項６に記載のカードシステム。

【請求項９】前記ＩＣカードは、当該ＩＣカードに記憶されているアプリケーションの削除に伴い、削除対象のアプリケーションに関する削除証明書を作成し、前記削除対象のアプリケーションの供給元の供給センタに供給し、

前記供給センタは、前記ＩＣカードからの削除証明書を前記カード発行センタに送信する、

ことを特徴とする請求項６乃至８のいずれか１項に記載のカードシステム。

【請求項１０】カード発行センタにより発行されたＩＣカードに、供給センタにより供給されるアプリケーションを記憶するカードシステム用のＩＣカードであって、

前記ＩＣカードは、前記供給センタが前記カード発行センタから取得した認証情報を受け取って、該認証情報の正当性をチェックし、チェック結果が正常を示す場合、

前記供給センタからのアプリケーションを当該ＩＣカードの所定領域に記憶し、チェック結果がエラーを示す場合、所定のエラー処理を行う、

ことを特徴とするＩＣカード。

【請求項１１】コンピュータを、カード発行センタにより発行され、供給センタにより供給されるアプリケーションを記憶するＩＣカードとして機能させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体であって、

該コンピュータを、

前記カード発行センタにより供給が許可されたアプリケーションに関する許可テーブルを記憶する手段、

前記供給センタから供給されたアプリケーションが前記許可テーブルに登録されているか否かを判別する手段、

前記判別手段により前記アプリケーションが前記許可テーブルに登録されていると判別された場合、該アプリケーションを当該ＩＣカードの所定領域に記憶する手段、

前記判別手段により前記アプリケーションが前記許可テーブルに登録されていないと判別された場合、所定のエラー処理を行う手段、

として機能させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体。

【請求項１２】コンピュータを、カード発行センタにより発行され、供給センタにより供給されるアプリケーションを記憶するＩＣカードとして機能させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体であって、

該コンピュータを、

前記供給センタが前記カード発行センタから取得した認証情報を受け取る手段、

前記認証情報の正当性をチェックする手段、

前記チェック結果が正常を示す場合、前記供給センタからのアプリケーションを当該ＩＣカードの所定領域に記憶する手段、

前記チェック結果がエラーを示す場合、所定のエラー処理を行う手段、

として機能させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、カード発行センタにより発行されたＩＣカードに、アプリケーションの供給を行う供給センタにより供給されるアプリケーションを記憶するカードシステム等に関する。

【０００２】

【従来の技術】例えばカード発行者が各利用者に対して発行したＩＣカードに、アプリケーションの供給者（サービス提供者）がカード用アプリケーションを供給して、ＩＣカードの多目的利用を図るカードシステムが知られている。このようなシステムでは、例えば、利用者

は所望のアプリケーションを自己のＩＣカードにダウンロードし、ＩＣカードに組み込まれたアプリケーションを実行させることにより、サービス提供者による所定のサービスを受けることができる。

【０００３】

【発明が解決しようとする課題】上記のようなカードシステムでは、例えば不正なサービス提供者によるＩＣカードへのアプリケーションの供給を防止し、安全にアプリケーションの供給が受けられる仕組みが必要とされている。

【０００４】また、システムの安全性を保持する観点からアプリケーションの供給者（サービス提供者）の認証処理を行う場合、その認証処理が複雑化・長時間化してしまうと、システムのレスポンスを低下させてしまうおそれがある。

【０００５】また、カード発行者により各ＩＣカードへのアプリケーションの供給状況が正確に把握され、例えば各サービス提供者への適正な課金管理が実現されること等が業界において望まれている。

【０００６】本発明は、上述した事情に鑑みてなされたもので、アプリケーションの供給を安全に行うことができるカードシステム等を提供することを目的とする。また、本発明は、アプリケーションの供給者の認証処理の複雑化・長時間化を防止することができるカードシステム等を提供することを他の目的とする。また、本発明は、ＩＣカードへのカード用アプリケーションの登録状況の管理が可能なシステム等を提供することを他の目的とする。

【０００７】

【課題を解決するための手段】上記目的を達成するため、本発明の第１の観点に係るカードシステムは、カード発行センタにより発行されたＩＣカードに、供給センタにより供給されるアプリケーションを記憶するカードシステムであって、前記ＩＣカードは、前記カード発行センタにより供給が許可されたアプリケーションに関する許可テーブルを記憶し、前記供給センタから供給されたアプリケーションが前記許可テーブルに登録されているか否かを判別し、前記アプリケーションが前記許可テーブルに登録されている場合、該アプリケーションを当該ＩＣカードの所定領域に記憶し、前記アプリケーションが前記許可テーブルに登録されていない場合、所定のエラー処理を行う。

【０００８】このような構成によれば、ＩＣカードに予めカード発行センタが許可したアプリケーションに関する許可テーブルを格納しておき、ＩＣカードにアプリケーションをダウンロードする際に、そのアプリケーションの正当性を許可テーブルを参照してチェックする。これにより、ダウンロードする度にカード発行センタにアプリケーションの正当性を問い合わせることなく、カード内でその正当性をチェックすることができるため、安

全性が高く、短時間での認証が可能なカードシステムを実現することができる。

【０００９】前記許可テーブルには、各前記アプリケーションについて、当該アプリケーション基づいて導出されるチェック情報がそれぞれ設定されてもよく、前記ＩＣカードは、前記供給センタからのアプリケーションの供給に応答し、前記供給されたアプリケーションに基づいてチェック情報を導出し、前記許可テーブルに設定されている該当するアプリケーションのチェック情報と照合してもよく、前記チェック情報が合致する場合には、前記供給されたアプリケーションを当該ＩＣカードの所定領域に記憶してもよく、前記チェック情報が合致しない場合には、所定のエラー処理を行ってもよい。

【００１０】前記チェック情報はハッシュ値を含んでもよい。

【００１１】前記許可テーブルには、管理機関による署名が付与されていてもよい。これにより、許可テーブルを用いてアプリケーションのチェックを行うことは、カード発行センタと管理機関の両方からの許可を確認することと実質的に同意となるため、さらにシステムの安全性を高めることができる。また、第三者的な管理機関による署名を付与することで、例えばカード発行元とアプリケーション供給者（サービス提供者）の共同による不正行為等を防止することができる。

【００１２】また、本発明の第２の観点に係るＩＣカードは、カード発行センタにより発行されたＩＣカードに、供給センタにより供給されるアプリケーションを記憶するカードシステム用のＩＣカードであって、前記カード発行センタにより供給が許可されたアプリケーションに関する許可テーブルを記憶し、前記供給センタから供給されたアプリケーションが前記許可テーブルに登録されているか否かを判別し、前記アプリケーションが前記許可テーブルに登録されている場合、該アプリケーションを当該ＩＣカードの所定領域に記憶し、前記アプリケーションが前記許可テーブルに登録されていない場合、所定のエラー処理を行う、ことを特徴とする。

【００１３】また、本発明の第３の観点に係るカードシステムは、カード発行センタにより発行されたＩＣカードに、供給センタにより供給されるアプリケーションを記憶するカードシステムであって、前記供給センタは、前記カード発行センタから認証情報を取得し、取得した前記認証情報とアプリケーションを前記ＩＣカードに供給し、前記ＩＣカードは、前記供給センタからの前記認証情報の正当性をチェックし、チェック結果が正常を示す場合、前記供給センタからのアプリケーションを当該ＩＣカードの所定領域に記憶し、チェック結果がエラーを示す場合、所定のエラー処理を行う、ことを特徴とする。

【００１４】このような構成によれば、ＩＣカードにアプリケーションを供給する時にはカード発行センタにより発行される認証情報が必要とされる。これにより、カード発行センタから認証情報を取得していないサービス提供サーバによるＩＣカードへのアプリケーションの登録を排除し、安全なカードシステムを提供することができる。

【００１５】前記供給センタは、ＩＣカードにアプリケーションを供給するとき、アプリケーションの供給先のＩＣカードからカード識別符号を取得し、取得した前記カード識別符号とアプリケーション識別符号を前記カード発行センタに供給してもよく、前記カード発行センタは、前記アプリケーション識別符号に基づくアプリケーションに関する情報を、前記カード識別符号により特定されるＩＣカードの鍵で暗号化したものを前記認証情報として前記供給センタに供給してもよく、前記ＩＣカードは、当該ＩＣカードの鍵を用いて前記認証情報の正当性をチェックしてもよい。

【００１６】また、供給センタは、ＩＣカードにアプリケーションを供給するとき、アプリケーションの供給先のＩＣカードから乱数を取得し、取得した乱数とアプリケーション識別符号を前記カード発行センタに供給してもよく、前記カード発行センタは、前記乱数と前記アプリケーション識別符号に基づくアプリケーションに関する情報を当該カード発行センタの鍵で暗号化したものを前記認証情報として前記供給センタに供給してもよく、前記ＩＣカードは、乱数を生成して前記供給センタに供給し、前記供給センタから供給された前記認証情報の正当性を前記カード発行センタの鍵を用いてチェックしてもよい。

【００１７】前記ＩＣカードは、当該ＩＣカードに記憶されているアプリケーションの削除に伴い、削除対象のアプリケーションに関する削除証明書を作成し、前記削除対象のアプリケーションの供給元の供給センタに供給してもよく、前記供給センタは、前記ＩＣカードからの削除証明書を前記カード発行センタに送信してもよい。

【００１８】これにより、アプリケーションがＩＣカードに供給される度に供給センタがカード発行センタから認証情報を取得するため、カード発行センタは、各ＩＣカードへアプリケーションが供給されたことを確実に把握することができる。また、ＩＣカードがアプリケーションの削除についての証明書を供給センタに対して発行し、供給センタがその証明書をカード発行センタに提出することにより、カード発行センタは、各ＩＣカードからアプリケーションが削除されたことを確実に把握することができる。また、カード発行センタは、各ＩＣカードについて、アプリケーションの登録及び削除を確実に把握できるため、供給センタに対して適正な課金管理を行うことができる。

【００１９】また、本発明の第４の観点に係るＩＣカードは、カード発行センタにより発行されたＩＣカードに、供給センタにより供給されるアプリケーションを記

憶するカードシステム用のＩＣカードであって、前記ＩＣカードは、前記供給センタが前記カード発行センタから取得した認証情報を受け取って、該認証情報の正当性をチェックし、チェック結果が正常を示す場合、前記供給センタからのアプリケーションを当該ＩＣカードの所定領域に記憶し、チェック結果がエラーを示す場合、所定のエラー処理を行う、ことを特徴とする。

【０００９】また、本発明の第５の観点に係る記録媒体は、コンピュータを、カード発行センタにより発行され、供給センタにより供給されるアプリケーションを記憶するＩＣカードとして機能させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体であって、該コンピュータを、前記カード発行センタにより供給が許可されたアプリケーションに関する許可テーブルを記憶する手段、前記供給センタから供給されたアプリケーションが前記許可テーブルに登録されているか否かを判別する手段、前記判別手段により前記アプリケーションが前記許可テーブルに登録されていると判別された場合、該アプリケーションを当該ＩＣカードの所定領域に記憶する手段、前記判別手段により前記アプリケーションが前記許可テーブルに登録されていないと判別された場合、所定のエラー処理を行う手段、として機能させるためのプログラムを記録する。

【００２１】また、本発明の第６の観点に係る記録媒体は、コンピュータを、カード発行センタにより発行され、供給センタにより供給されるアプリケーションを記憶するＩＣカードとして機能させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体であって、該コンピュータを前記供給センタが前記カード発行センタから取得した認証情報を受け取る手段、前記認証情報の正当性をチェックする手段、前記チェック結果が正常を示す場合、前記供給センタからのアプリケーションを当該ＩＣカードの所定領域に記憶する手段、前記チェック結果がエラーを示す場合、所定のエラー処理を行う手段、として機能させるためのプログラムを記録する。

【００２２】

【発明の実施の形態】以下、本発明の実施の形態に係るカードシステムを図面を参照して説明する。このカードシステムは、カード発行者が利用者に対して発行したＩＣカードに、アプリケーションの供給者（サービス提供者）により供給される種々のカード用アプリケーションをダウンロードして組み込むためのものである。

【００２３】（第１の実施形態）本発明の第１の実施形態に係るカードシステムのシステム構成図を図１に示す。図示されるように、このカードシステムは、カード発行センタ１と、管理センタ２と、カード処理端末３と、ＩＣカード４と、各サービス提供者のサービス提供サーバ５と、を備える。

【００２４】カード発行センタ１は、利用者に対するＩＣカード３の発行等を行う。このＩＣカード３の発行では、カード発行センタ１は、各サービス提供サーバ５が配信するカード用アプリケーションに基づいて、カード用アプリケーションに関する所定のテーブル（許可テーブル）を作成し、その許可テーブルに対して管理センタ２から署名の付与を受ける。そして、署名が付与された許可テーブルと所定のカード情報（カードＩＤ等）を発行対象のＩＣカード３に記録して発行する。

【００２５】カード発行センタ１により生成される許可テーブルには、例えば図２に示すように、各サービス提供サーバ５が提供するカード用アプリケーションについて、アプリケーションＩＤ、ハッシュ値等の情報が、サービス提供サーバ５を識別するためのサービス提供者ＩＤ毎に設定される。このハッシュ値は、例えばカード用アプリケーションのプログラム等、カード用アプリケーション毎に一意の情報に基づいて生成される。

【００２６】管理センタ２は、カード発行センタ１からの要求に応じて、カード発行センタ１が生成した許可テーブルに対して署名（管理者署名）を付与する。

【００２７】カード処理端末３は、ＩＣカードリーダ／ライタ等を備え、主にＩＣカード４とサービス提供サーバ５との間のデータ送受信等を行う。例えば、カード処理端末３は、利用者から入力されたカード用アプリケーションのダウンロードの要求をカードリーダ／ライタを介してＩＣカード４に通知し、これに応じてＩＣカード４から受信したカードＩＤ等をカード用アプリケーションのダウンロード要求とともにサービス提供サーバ５に送信する。また、サービス提供サーバ５から受信したカード用アプリケーションをカードリーダ／ライタを介してＩＣカード４に送信等する。

【００２８】ＩＣカード４は、ＭＰＵ、ＲＯＭ、ＲＡＭ、ＥＥＰＲＯＭ等を有するＩＣチップを備え、このＩＣチップは、例えば図３に示すように、ＭＰＵがＲＯＭ等に記憶されるプログラムを実行することにより実現される制御部４１とメモリ４２と入出力制御部４３とを備える。

【００２９】制御部４１は、カード処理端末３からの所定の通知に応じて、メモリに記憶されるカードＩＤ等をカード処理端末３に送信する。そして、制御部４１は、ダウンロードされたカード用アプリケーションをカード処理端末３から受信すると、そのカード用アプリケーションのハッシュ値を作成する。そして、受信したカード用アプリケーションのアプリケーションＩＤと、作成したハッシュ値を、メモリ４２に記憶されている許可テーブルの設定値と照合する。

【００３０】比較したアプリケーションＩＤ及びハッシュ値が一致する場合には、制御部４１は、そのカード用アプリケーションが予めカード発行センタ１に許可されたものであるとして、メモリ４２におけるカード用アプリケーションを記憶するための記憶領域に、受信したカ

ード用アプリケーションを記憶する。

【００３１】また、比較したアプリケーションＩＤ及びハッシュ値が一致しない場合には、制御部４１は、カード発行センタ１が許可したカード用アプリケーションでないと判別し、カード用アプリケーションを所定の記憶領域に記憶することなく、カード処理端末３にエラー信号を送信して、エラー表示させる等の所定のエラー処理を行う。

【００３２】メモリ４２は、許可テーブル、カード情報（カードＩＤ等）、カード用アプリケーション等を記憶する。入出力制御部４３は、カード処理端末３とのデータ通信を制御する。

【００３３】サービス提供サーバ５は、ＩＣカード４へのカード用アプリケーションの提供等を行うためのサーバである。サービス提供サーバ５は、カード処理端末３からのカード用アプリケーションのダウンロード要求に応答して、該当するカード用アプリケーションを図示せぬ記憶部から読み出して、要求元のカード処理端末３に送信する。

【００３４】次に、この第１の実施形態に係るシステムにおいて、ＩＣカード４にカード用アプリケーションを登録する場合の処理を図４を参照して説明する。例えば、ある利用者は、カード処理端末３にＩＣカード４をセットして、サービス提供サーバ５（サービス提供者ＩＤ：ＢＢＢ）が提供するカード用アプリケーション（アプリケーションＩＤ：１２３）のダウンロード要求を入力する。これに応じて、カード処理端末３はダウンロードの要求の入力をＩＣカード４に通知して、カードＩＤ等を取得し、アプリケーションＩＤ「１２３」のカード用アプリケーションのダウンロード要求とともにサービス提供サーバ５に送信する（ステップＳ１、Ｓ２）。

【００３５】ダウンロード要求を受信したサービス提供サーバ５は、該当するアプリケーションＩＤ「１２３」のカード用アプリケーションを読み出して、カード処理端末３を介してＩＣカード４に送信する（ステップＳ３）。

【００３６】ＩＣカード４は、受信したカード用アプリケーションについてハッシュ値（例えば、「２３」）を生成する（ステップＳ４）。そして、受信したカード用アプリケーションのアプリケーションＩＤ「１２３」と、生成したハッシュ値「２３」が、メモリ４２に記憶されているサービス提供者ＩＤ「ＢＢＢ」の許可テーブルの設定値と合致するかを判別する（ステップＳ５）。

【００３７】比較したアプリケーションＩＤ及びハッシュ値が合致する場合、ＩＣカード４は受信したカード用アプリケーションを、カード発行センタ１から許可されている正当なアプリケーションであるとして、メモリ４２のカード用アプリケーション用領域に格納する（ステップＳ６）。

【００３８】また、例えば、比較したアプリケーションＩＤとハッシュ値が許可テーブルの設定値と合致しない場合には、ＩＣカード４は、受信したカード用アプリケーションを、カード発行センタ１からの許可を受けていない不当なアプリケーションであるとして、例えば、そのカード用アプリケーションをカード用アプリケーション用の記憶領域に記憶することなく消去して、カード処理端末３にエラー信号を送信する等の所定のエラー処理を実行する（ステップＳ７）。

【００３９】このようにして、ＩＣカード４に予めカード発行センタ１が許可したカード用アプリケーションに関する許可テーブルを格納しておき、ＩＣカード４にカード用アプリケーションをダウンロードする際に、そのカード用アプリケーションの正当性を許可テーブルを参照してチェックする。これにより、ダウンロードする度にカード発行センタ１にカード用アプリケーションの正当性を問い合わせることなく、カード内でその正当性をチェックすることができるため、安全性が高く、短時間での認証が可能なカードシステムを実現することができる。

【００４０】また、ＩＣカード４に格納される許可テーブルには、管理センタ２による管理者としての署名が付与されているため、この許可テーブルを用いてカード用アプリケーションのチェックを行うことは、カード発行センタ１と管理センタ２の両方からの許可を確認することと実質的に同意である。よって、さらにシステムの安全性を高めることができる。また、第三者的な管理センタ２による署名を付与することで、例えばカード発行元とサービス提供者の共同による不正行為等を防止することができる。

【００４１】また、管理センタ２を除いたシステム構成としてもよい。この場合、許可テーブルに第三者に管理センタ２による署名は付与されないが、上記説明のように、ＩＣカード４内で許可テーブルに基づくチェックは行うため、安全性が高く、短時間での認証が可能なカードシステムを実現することができる。

【００４２】また、各サービス提供者が提供するカード用アプリケーションが追加される場合や新たなサービス提供者が追加される場合等に、新たな許可テーブルをカード発行センタ１がカード処理端末３を介してＩＣカード４に供給するようにしてもよい。

【００４３】また、許可テーブルに記憶するチェック用データはハッシュ値に限定されない。例えばカード用アプリケーションに対して一意な数値、データ等を導出できる任意の関数を用いても良い。

【００４４】また、サービス提供者のカード用アプリケーションを記憶部に格納し、カードリーダライタを備えるサービス提供装置を用いても良い。この場合、利用者は、サービス提供装置にＩＣカード４をセットして、所望のカード用アプリケーションのＩＣカード４への書込要求を入力する。この入力に応じて、サービス提供装置

(7)

は、指定されたカード用アプリケーションを記憶部から読み出して、ＩＣカード４に渡す。ＩＣカード４は、上記説明と同様にして、許可テーブルに基づくカード用アプリケーションのチェックを行い、その正当性を確認した場合にはメモリ４２の所定記憶領域に記録し、不当であると判別した場合には受け取ったアプリケーションを消去する等のエラー処理を行う。

【００４５】（第２の実施形態）本発明の第２の実施形態に係るカードシステムのシステム構成図を図５に示す。図示されるように、このカードシステムは、カード発行センタ６と、カード処理端末７と、ＩＣカード８と、各サービス提供者のサービス提供サーバ９と、を備える。

【００４６】カード発行センタ６は、利用者に対するＩＣカード８の発行等を行う。カード発行センタ６は、発行対象の各ＩＣカード８のメモリに、カード毎に一意の暗号鍵（カード用秘密鍵）を記録する。また、カード発行センタ６は、例えば図６に示すような、各ＩＣカード８のカードＩＤと暗号鍵（カード用公開鍵）を対応付ける鍵テーブルを記憶する。また、カード発行センタ６は、各サービス提供サーバ９が提供するカード用アプリケーションについて、アプリケーションＩＤと、そのカード用アプリケーションに基づいて生成されたハッシュ値が対応付けられているテーブルを記憶する。

【００４７】カード発行センタ６は、サービス提供サーバ９から、例えばカードＩＤとサービス提供者ＩＤとアプリケーションＩＤを含む鍵要求情報を受信すると、鍵要求情報に含まれるアプリケーションＩＤに対応するハッシュ値を読み出す。そして、鍵要求情報に含まれるカードＩＤに対応する暗号鍵（カード用公開鍵）を鍵テーブルから読み出し、その暗号鍵で先に取得したハッシュ値を暗号化し、暗号化されたハッシュ値に、カード発行センタ６による署名を付与して要求元のサービス提供サーバ９に送信する。

【００４８】また、カード発行センタ６は、サービス提供サーバ９から受信した鍵要求情報に基づいて、例えば図７に示すような、サービス提供者ＩＤ、カードＩＤ、アプリケーションＩＤ、登録日時等を含む課金情報を生成して記憶する。そして、この課金情報に基づいて、ＩＣカード８にカード用アプリケーションを供給するサービス提供者に対して課金を行う。課金の方法は任意であり、例えば、１アプリケーション毎に、カードへの記録時間が所定時間経過する毎に所定金額がアプリケーション提供元に課金されるようにしてもよい。

【００４９】また、カード発行センタ６は、サービス提供サーバ９から、サービス提供者ＩＤとアプリケーションの削除に関する証明書を受信すると、課金情報を参照して、受信データに該当する課金情報を特定し、その課金情報に対して、例えばアプリケーションの削除日時等の情報を設定する。なお、この証明書は、ＩＣカード８からカード用アプリケーションが削除された場合にＩＣカード８によりサービス提供サーバ９に対して発行される情報であり、例えば、削除されたアプリケーションＩＤとカードＩＤ等を含む。この証明書は、例えばＩＣカード８の秘密鍵で署名がなされていてもよい。この場合、カード発行センタ６は、ＩＣカード８の公開鍵を用いて署名を確認することにより、証明書の正当性を確認する。

【００５０】カード処理端末７は、ＩＣカードリーダ／ライタ等を備え、主にＩＣカード８とサービス提供サーバ９との間のデータ送受信等を行う。例えば、カード処理端末７は、利用者から入力されたカード用アプリケーションのダウンロード又は削除の要求等をカードリーダ／ライタを介してＩＣカード８に通知し、これに応じてＩＣカード８から受信したカードＩＤをカード用アプリケーションのダウンロード要求又は削除要求通知等とともにサービス提供サーバ９に送信する。また、カード処理端末７は、サービス提供サーバ９から受信したアクセス要求、暗号化されたハッシュ値、カード用アプリケーション等をカードリーダ／ライタを介してＩＣカード４に送信する。

【００５１】ＩＣカード８は、ＭＰＵ、ＲＯＭ、ＲＡＭ、ＥＥＰＲＯＭ等を有するＩＣチップを備え、このＩＣチップは、例えば図８に示すように、ＭＰＵがＲＯＭ等に記憶されるプログラムを実行することにより実現される制御部８１とメモリ８２と入出力制御部８３とを備える。

【００５２】制御部８１は、カード処理端末７からの、ダウンロードの要求、カード用アプリケーションの削除の要求等が入力されたことの通知に応じて、メモリに記憶されるカードＩＤ等をカード処理端末７に送信する。

【００５３】また、制御部８１は、サービス提供サーバ９からの、ＩＣカード８へのアクセス要求（書込要求）と暗号化されたハッシュ値とカード用アプリケーション等をカード処理端末７を介して受信すると、暗号化されたハッシュ値に付与されている署名の検証を行う。そして、署名が正しければ、メモリ８２に記憶されている暗号鍵（カード用秘密鍵）を用いて、暗号化されたハッシュ値を復号化する。次に、復号化したハッシュ値を、受信したカード用アプリケーションに基づいて作成したハッシュ値と照合する。そして、比較したハッシュ値が一致する場合には、制御部８１は、メモリ８２におけるカード用アプリケーションを記憶するための記憶領域に、受信したカード用アプリケーションを記憶する。また、比較したハッシュ値が一致しない場合には、制御部８１は、カード用アプリケーションを所定の記憶領域に記憶することなく、カード処理端末７にエラー信号を送信して、エラー表示させる等の所定のエラー処理を行う。

【００５４】また、制御部８１は、サービス提供サーバ９からの、カード用アプリケーションの削除要求等をカ

ード処理端末７を介して受信すると、指定されたカード用アプリケーションをメモリ８２から削除する。そして、削除したカード用アプリケーションのアプリケーションＩＤ、そのＩＣカード８のカードＩＤ等を含む証明書をカード処理端末７を介してサービス提供サーバ９に送信する。なお、この証明書にＩＣカード８の秘密鍵を用いた署名を付与してもよい。

【００５５】メモリ８２は、暗号鍵（カード用秘密鍵）、カード発行者の公開鍵、カード情報（カードＩＤ等）、カード用アプリケーション等を記憶する。入出力制御部８３は、カード処理端末７とのデータ通信を制御する。

【００５６】サービス提供サーバ９は、ＩＣカード８へのカード用アプリケーションの提供等を行うためのサーバである。サービス提供サーバ９は、カード処理端末７からの、カード用アプリケーションのダウンロード要求に応答して、例えば、ダウンロード要求とともに受信したカードＩＤと、要求されたカード用アプリケーションのアプリケーションＩＤと、サービス提供者ＩＤを含む鍵要求情報を生成して、カード発行センタ６に送信し、暗号化されたハッシュ値をカード発行センタ６から受信する。そして、サービス提供サーバ９は、ダウンロード要求に該当するカード用アプリケーションを図示せぬ記憶部から読み出し、暗号化されたハッシュ値と所定のアクセス要求（書込要求）とともにカード処理端末７を介してＩＣカード８に送信する。

【００５７】また、サービス提供サーバ９は、カード処理端末７からのカード用アプリケーションの削除要求通知に応答して、指定されたアプリケーションの削除要求をカード処理端末７を介してＩＣカード８に送信する。そして、ＩＣカード８からの証明書をカード処理端末７を介して受信し、この証明書をカード発行センタ６に送信する。

【００５８】次に、この第２の実施形態に係るシステムにおいて、ＩＣカード８にカード用アプリケーションを登録する場合の処理を図９を参照して説明する。例えば、ある利用者は、カード処理端末７にＩＣカード８（カードＩＤ：３２３２）をセットして、サービス提供サーバ９が提供するカード用アプリケーションのダウンロード要求を入力する。これに応じて、カード処理端末７はダウンロードの要求の入力をＩＣカード８に通知して、カードＩＤ「３２３２」等を取得し、カード用アプリケーションのダウンロード要求（ダウンロード対象のアプリケーションＩＤを含む）とともにサービス提供サーバ９に送信する（ステップＳ１１、Ｓ１２）。

【００５９】ダウンロード要求を受信したサービス提供サーバ９は、受信したカードＩＤ「３２３２」と、要求されたカード用アプリケーションのアプリケーションＩＤと、サービス提供者ＩＤを含む鍵要求情報を生成して、カード発行センタ６に送信する（ステップＳ１３）。

【００６０】カード発行センタ６は、鍵要求情報の受信に応答し、この受信データに含まれるアプリケーションＩＤに対応するハッシュ値を読み出す。また、カードＩＤ「３２３２」に対応する暗号鍵「１２１２」を鍵テーブルから読み出して、その暗号鍵でハッシュ値を暗号化し、暗号化されたハッシュ値にカード発行センタ６の秘密鍵を用いた署名を付与して要求元のサービス提供サーバ９に送信する（ステップＳ１４）。また、カード発行センタ６は、サービス提供サーバ９からの受信データを用いて課金情報を生成して記憶する（ステップＳ１５）。そして、課金情報に基づいてサービス提供者がカードＩＤ「３２３２」にカード用アプリケーションを提供することに対して課金を行う。

【００６１】また、サービス提供サーバ９は、カード発行センタ６から受信した暗号化されたハッシュ値と、要求されたカード用アプリケーションと、アクセス要求（書込要求）を、カード処理端末７を介してＩＣカード８に送信する（ステップＳ１６）。

【００６２】ＩＣカード８は、受信した暗号化されたハッシュ値に付与されている署名について、カード発行センタの公開鍵を用いて検証する。署名が正しければ、暗号鍵（カード用秘密鍵）を用いて暗号化されたハッシュ値を復号化する。そして、復号化されたハッシュ値が、受信したカード用アプリケーションに基づいて作成したハッシュ値と合致するかを判別する（ステップＳ１７）。

【００６３】比較したハッシュ値が合致する場合、ＩＣカード８は、送信元の正当性を確認したとして、受信したカード用アプリケーションを、メモリ８２のカード用アプリケーション用領域に格納する（ステップＳ１８）。

【００６４】また、比較したハッシュ値が合致しない場合又は署名が不当なものである場合等には、ＩＣカード８は、例えば、そのカード用アプリケーションをカード用アプリケーション用の記憶領域に記憶することなく消去して、カード処理端末７にエラー信号を送信する等の所定のエラー処理を実行する（ステップＳ１９）。

【００６５】次に、この第２の実施形態に係るシステムにおいて、ＩＣカード８からカード用アプリケーションを削除する場合の処理を図１０を参照して説明する。例えば利用者は、カード処理端末７にＩＣカード８（カードＩＤ：３２３２）をセットして、ＩＣカード８に記憶されているカード用アプリケーションの削除要求を入力する。これに応じて、カード処理端末７はアプリケーションの削除の要求の入力をＩＣカード８に通知して、カードＩＤ「３２３２」等を取得し、カード用アプリケーションの削除要求通知（削除対象のアプリケーションＩＤを含む）とともにサービス提供サーバ９に送信する（ステップＳ２１、Ｓ２２）。

【００６６】削除要求を受信したサービス提供サーバ９は、指定されたカード用アプリケーションを削除するためのアクセス要求（削除要求）をカード処理端末７を介してＩＣカード８に送信する（ステップＳ２３）。これに応じて、ＩＣカード８は、指定されたカード用アプリケーションをメモリ８２から削除するとともに、このカード用アプリケーションを削除したことを示す証明書を作成する（ステップＳ２４、Ｓ２５）。そして、作成した証明書をカード処理端末７を介してサービス提供サーバ９に送信する（ステップＳ２６）。

【００６７】サービス提供サーバ９は、ＩＣカード８から受信した証明書をカード発行センタ６に送信する（ステップＳ２７）。カード発行センタ６は、受信した証明書からカード用アプリケーションが削除されたことを確認し、該当する課金情報にカード用アプリケーションの削除日時等を設定する（ステップＳ２８）。

【００６８】このようにして、ＩＣカード８にカード用アプリケーションを登録する時には、カード用アプリケーションの情報をＩＣカード８に固有の鍵で暗号化したものにカード発行センタ６が署名をしたものを必要とする。これにより、そのカードにしか有効でない認証用情報がカード発行センタ６により生成されるため、不正なサービス提供サーバ９によるＩＣカード８へのカード用アプリケーションの登録を排除し、安全なカードシステムを提供することができる。また、ＩＣカード８によりカード用アプリケーションの削除についての証明書を発行させて、サービス提供サーバ９にその証明書を提出させること等により、カード発行センタ６では、各ＩＣカード８へのカード用アプリケーションに登録及び削除を確実に把握できるため、適正な課金管理を行うことができる。

【００６９】また、ＩＣカード８のカード用アプリケーションを削除する場合も、登録の場合と同様に、カード発行センタ６による認証を必要とするようにしてもよい。この場合、サービス提供サーバ９は、登録の場合と同様に、カード発行センタ６から暗号化されたハッシュ値と署名を取得して、カード用アプリケーションの削除要求とともに暗証鍵をＩＣカード８に対して送信する。

【００７０】また、サービス提供者のカード用アプリケーションを記憶部に格納し、カードリーダライタを備えるサービス提供装置を用いても良い。この場合、利用者は、サービス提供装置にＩＣカード８をセットして、所望のカード用アプリケーションのＩＣカード８への書込要求を入力する。この入力に応じて、サービス提供装置は、カードＩＤとアプリケーションＩＤをカード発行センタ６に送信して、これに対する暗号化されたハッシュ値と署名をカード発行センタ６から取得し、指定されたカード用アプリケーションとともにＩＣカード８に渡す。ＩＣカード８は、上記説明と同様にして、署名及びハッシュ値のチェックを行い、その正当性を確認した場合にはメモリ８２の所定記憶領域にカード用アプリケーションを記録し、不当であると判別した場合には受け取ったアプリケーションを消去する等のエラー処理を行う。

【００７１】また、カード発行センタ６において、ＩＣカード８の暗号鍵で暗号化するものはアプリケーションＩＤに対応するハッシュ値に限定されず、そのカード用アプリケーションに一意な情報であればよい。例えば、アプリケーションＩＤをＩＣカード８の暗号鍵で暗号化したものに署名を付与して、サービス提供サーバ９に供給するようにしてもよい。この場合、ＩＣカード８は、署名を検証した後、暗号化されたアプリケーションＩＤを暗号鍵で復号化し、受信したカード用アプリケーションのアプリケーションＩＤであるかを判別する。

【００７２】また、カード用アプリケーションのＩＣカード８への登録に先立ってＩＣカード８が乱数を生成し、その乱数をカード発行センタ６による署名の対象に含めるようにしてもよい。この場合、例えば図１１に示すように、サービス提供サーバ９は、ＩＣカード８に対して、乱数の生成を要求する（ステップＳ３１）。これに応じて、ＩＣカード８は、乱数を生成し、生成した乱数等をサービス提供サーバ９に送信する（ステップＳ３２）。サービス提供サーバ９は、受信した乱数等と、ダウンロード対象のカード用アプリケーションのアプリケーションＩＤ等をカード発行センタ６に送信する（ステップＳ３３）。

【００７３】これに応じて、カード発行センタ６は、受信したアプリケーションＩＤに対応するハッシュ値を読み出す。そして、読み出したハッシュ値と受信した乱数をカード発行センタ６の秘密鍵で暗号化した許可情報を生成し、要求元のサービス提供サーバ９に送信する（ステップＳ３４）また、カード発行センタ６は、サービス提供者に対する課金を行う。サービス提供サーバ９は、カード発行センタ６から受信した許可情報と、要求されたカード用アプリケーションをアクセス要求とともにＩＣカード８に送信する（ステップＳ３５）。

【００７４】ＩＣカード８は、受信した許可情報をカード発行センタ６の公開鍵で復号化して、ハッシュ値と乱数を取得する。そして、取得した乱数を、自己が生成した乱数と照合する。また、ＩＣカード８は、受信したカード用アプリケーションに基づいて作成した作成したハッシュ値を、受信したハッシュ値と照合する（ステップＳ３６）。

【００７５】そして、乱数の照合結果とハッシュ値の照合結果の双方が正常である場合には、受信したカード用アプリケーションをメモリ８２の所定領域に格納し（ステップＳ３７）、いずれかの照合結果がエラーを示す場合には、そのカード用アプリケーションを所定領域に記憶することなく消去して、カード処理端末７にエラー信号を送信する等の所定のエラー処理を行う（ステップＳ

３８）。

【００７６】このようにして、乱数を用いることにより、１回限り有効な認証用情報が作成されるため、セキュリティのレベルを高めることができる。また、この例においても、カード発行センタ６における暗号化の対象はアプリケーションＩＤに対応するハッシュ値に限定されず、そのカード用アプリケーションに一意な情報であればよい。例えば乱数とアプリケーションＩＤをカード発行センタ６に秘密鍵で暗号化したものを許可情報としてサービス提供サーバ９に供給するようにしてもよい。この場合、ＩＣカード８は、復号化して得た乱数についての照合とアプリケーションＩＤについての照合を行う。

【００７７】また、上記実施例において用いる暗号方式は秘密鍵暗号方式に限定されず、共通鍵暗号方式を用いてもよい。

【００７８】また、第１と第２の実施の形態におけるカード処理端末３、７は、携帯端末（携帯電話機）等を含む。

【００７９】なお、この発明のシステムは、専用のシステムによらず、通常のコンピュータシステムを用いて実現可能である。例えば、コンピュータに上述の動作を実行させるためのプログラムを格納した媒体（フロッピー（登録商標）ディスク、ＣＤ－ＲＯＭ等）から該プログラムをインストールすることにより、上述の処理を実行するカード発行センタ１、６、管理センタ２、カード処理端末２、７等を構成することができる。なお、上述の機能を、ＯＳが分担又はＯＳとアプリケーションの共同により実現する場合等には、ＯＳ以外の部分のみを媒体に格納してもよい。

【００８０】なお、搬送波にプログラムを重畳し、通信ネットワークを介して配信することも可能である。例えば、通信ネットワークの掲示板（ＢＢＳ）に該プログラムを掲示し、これをネットワークを介して配信してもよい。そして、このプログラムを起動し、ＯＳの制御下で、他のアプリケーションプログラムと同様に実行することにより、上述の処理を実行することができる。

【００８１】

【発明の効果】以上説明したように、本発明によれば、カード発行センタによる認証を受けていない供給センタによるＩＣカードへのアプリケーションの供給を排除し、安全なアプリケーションの供給を可能とする。

【図面の簡単な説明】

【図１】本発明の第１の実施形態に係るカードシステムのシステム構成図である。

【図２】許可テーブルを説明するための図である。

【図３】図１のカードシステムで使用されるＩＣカードの構成を説明するための図である。

【図４】図１のカードシステムにおいてＩＣカードにカード用アプリケーションを登録する場合の処理を説明するための図である。

【図５】本発明の第２の実施形態に係るカードシステムのシステム構成図である。

【図６】鍵テーブルを説明するための図である。

【図７】課金情報を説明するための図である。

【図８】図５のカードシステムで使用されるＩＣカードの構成を説明するための図である。

【図９】図５のカードシステムにおいてＩＣカードにカード用アプリケーションを登録する場合の処理を説明するための図である。

【図１０】図５のカードシステムにおいてＩＣカードからカード用アプリケーションを削除する場合の処理を説明するための図である。

【図１１】図５のカードシステムにおいてＩＣカードにカード用アプリケーションを登録する場合の処理の他の例を説明するための図である。

【符号の説明】

１、６　　カード発行センタ
２　　管理センタ
３、７　　カード処理端末
４、８　　ＩＣカード
５、９　　サービス提供サーバ
４１、８１　制御部
４２、８２　メモリ
４３、８３　入出力制御部

【図２】

許可テーブル

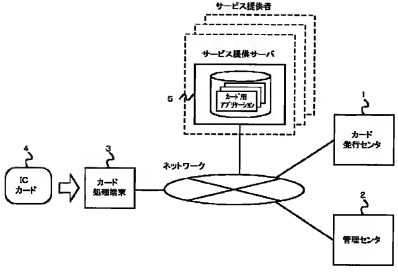
サービス提供者ID			
アプリケーションID	123	213	345
ハッシュ値	23	34	17
⋮	⋮	⋮	⋮

【図６】

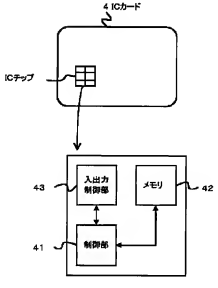
鍵テーブル

カードID	暗証鍵
9876	XXXXXX
5432	XXXXXX
⋮	⋮

【図１】



【図３】

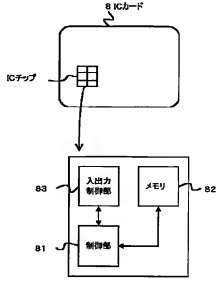


【図７】

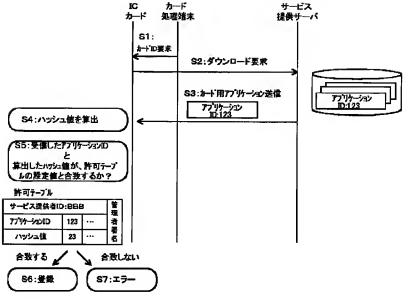
課金テーブル

サービス提供者ID	カードID	アプリケーションID	登録日時	…
876	1234	111	XXXX/XX/XX XX:XX	…
432	5678	222	XXXX/XX/XX XX:XX	…
⋮	⋮	⋮	⋮	⋮

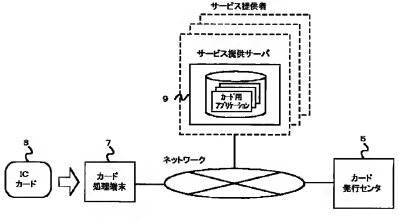
【図８】



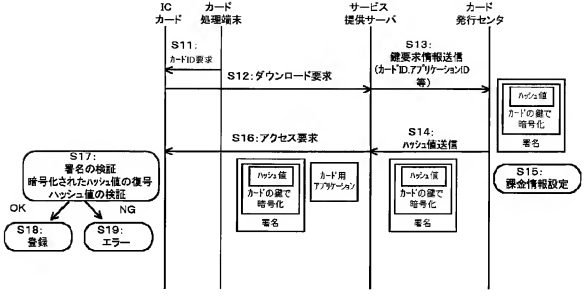
【図４】


ICカード
カード処理端末
サービス提供サーバ
S1：カードID要求
S2：ダウンロード要求
S3：カード用アプリケーション送信
アプリケーションID:123
アプリケーションID:123
S4：ハッシュ値を算出
S5：受信したアプリケーションIDと算出したハッシュ値が、許可テーブルの登録値と合致するか？
許可テーブル
サービス提供者ID:BBB
アプリケーションID
123
ハッシュ値
23
署名者名
合致する
合致しない
S6：登録
S7：エラー

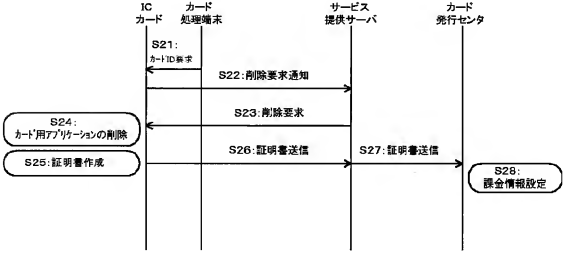
【図５】


サービス提供者
サービス提供サーバ
カード用アプリケーション
9
8
ICカード
7
カード処理端末
ネットワーク
5
カード発行センタ

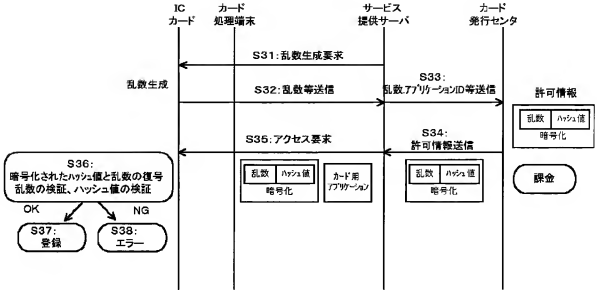
【図９】


IC
カード
カード
処理端末
サービス
提供サーバ
カード
発行センタ
S11:
カードID要求
S12:ダウンロード要求
S13:
鍵要求情報送信
(カードID,アプリケーションID
等)
ハッシュ値
カードの鍵で
暗号化
署名
S14:
ハッシュ値送信
S16:アクセス要求
S15:
課金情報設定
S17:
署名の検証
暗号化されたハッシュ値の復号
ハッシュ値の検証
ハッシュ値
カードの鍵で
暗号化
署名
カード用
アプリケーション
ハッシュ値
カードの鍵で
暗号化
署名
OK
NG
S18:
登録
S19:
エラー

【図１０】


IC
カード
カード
処理端末
サービス
提供サーバ
カード
発行センタ
S21:
カードID要求
S22:削除要求通知
S23:削除要求
S24:
カード用アプリケーションの削除
S25:証明書作成
S26:証明書送信
S27:証明書送信
S28:
課金情報設定

【図１１】



フロントページの続き

(51) Int. Cl.[7]	識別記号	F I	ﾃｰﾏｺｰﾄﾞ(参考)
Ｇ０６Ｋ 19/00		Ｇ０６Ｋ 19/00	Ｑ

(72)発明者 岡宮 俊一
東京都江東区豊洲三丁目３番３号 株式会社エヌ・ティ・ティ・データ内
(72)発明者 玉井 純
東京都江東区豊洲三丁目３番３号 株式会社エヌ・ティ・ティ・データ内
(72)発明者 冨永 洋
東京都江東区豊洲三丁目３番３号 株式会社エヌ・ティ・ティ・データ内
(72)発明者 高木 聡一郎
東京都江東区豊洲三丁目３番３号 株式会社エヌ・ティ・ティ・データ内

Ｆターム(参考) 5B035 AA06 AA13 BB09 CA29
5B058 KA11 KA31 KA33
5B076 BB06 FB02 FB09

[Document Name] Description

[Title of the Invention] A card system, an IC card, and a recording medium

[Claim(s)]

[Claim 1] Are the application supplied to the IC card published by the card issue center by the supply center the card system to memorize, and [said IC card] The permission table about the application with which supply was permitted by said card issue center is memorized. It is distinguished whether the application supplied from said supply center is registered into said permission table. The card system characterized by what this application is memorized to the predetermined field of the IC card concerned when said application is registered into said permission table, and predetermined error handling is performed for when said application is not registered into said permission table.

[Claim 2] About each aforementioned application, it is set to said permission table by the check information concerned by which application machine ****** derivation is carried out, respectively, and [said IC card] Answer supply of the application from said supply center, and check information is drawn based on said supplied application. When it compares with the check information on the applicable application set as said permission table and said check information agrees The card system according to claim 1 characterized by what predetermined error handling is performed for when said supplied application is memorized to the predetermined field of the IC card concerned and said check information does not agree.

[Claim 3] Said check information is a card system according to claim 2 characterized by what a hash value is included for.

[Claim 4] The card system according to claim 1 or 2 characterized by what the signature by a management organization is given to said permission table for.

[Claim 5] It is the IC card for card systems which memorizes the application supplied to the IC card published by the card issue center by the supply center. The permission table about the application with which supply was permitted by said card issue center is memorized. It is distinguished whether the application supplied from said supply center is registered into said permission table. The IC card characterized by what this application is memorized to the predetermined field of the IC card concerned when said application is registered into said permission table, and predetermined error handling is performed for when said application is not registered into said permission table.

[Claim 6] Are the application supplied to the IC card published by the card issue center by the supply center the card system to memorize, and [said supply center] Acquire attestation information from said card issue center, supply said attestation information and application which were acquired to said IC card, and [said IC card] The card system characterized by what the application from said supply center is memorized to the predetermined field of the IC card concerned when the justification of said attestation information from said supply center is checked and a check result shows normalcy, and predetermined error handling is performed for when a check result shows an error.

[Claim 7] When said supply center supplies application to an IC card, A card identification signal is acquired from the IC card of the supply place of application. Supply said card identification signal and application identification signal which were acquired to said card issue center, and [said card issue center] [the information about the application based on said application identification signal] It is the card system according to claim 6 which supplies said supply center by making into said attestation information what was enciphered with the key of the IC card specified by said card identification signal, and is characterized by what said IC card checks the justification of said attestation information for using the key of the IC card concerned.

[Claim 8] A supply center acquires a random number from the IC card of the supply place of application, when supplying application to an IC card. Supply the random number and application identification signal which were acquired to said card issue center, and [said card issue center] Said supply center is supplied by making into said attestation information what enciphered the information about the application based on said random number and said application identification signal with the key of the card issue center concerned. Said IC card is a card system according to claim 6 characterized by what the justification of said attestation information which generated the random number, supplied said supply center, and was supplied from said supply center is checked for using the key of said card

issue center.

[Claim 9] Said IC card is followed on deletion of the application memorized by the IC card concerned. Draw up the deletion certificate about the application for deletion, supply the supply center of the supply origin of the application for [said] deletion, and [said supply center] A card system given in any 1 clause of the Claims 6-8 characterized by what the deletion certificate from said IC card is transmitted for to said card issue center.

[Claim 10] Are the application supplied to the IC card published by the card issue center by the supply center the IC card for card systems to memorize, and [said IC card] The attestation information which said supply center acquired from said card issue center is received. The IC card characterized by what the application from said supply center is memorized to the predetermined field of the IC card concerned when the justification of this attestation information is checked and a check result shows normalcy, and predetermined error handling is performed for when a check result shows an error.

[Claim 11] It is the recording medium which recorded the program for making it function as an IC card which memorizes the application which is published by the card issue center and supplied by the supply center in a computer and in which computer reading is possible. A means to memorize the permission table about the application with which this computer was permitted to supply by said card issue center, A means to distinguish whether the application supplied from said supply center is registered into said permission table, When said application was registered into said permission table by said distinction means and it is distinguished, When said application was not registered into said permission table by means to memorize this application to the predetermined field of the IC card concerned, and said distinction means and it is distinguished, The recording medium which recorded the program for considering it as a means to perform predetermined error handling, and making it function and in which computer reading is possible.

[Claim 12] It is the recording medium which recorded the program for making it function as an IC card which memorizes the application which is published by the card issue center and supplied by the supply center in a computer and in which computer reading is possible. A means to receive the attestation information to which said supply center acquired this computer from said card issue center, When a means to check the justification of said attestation information, and said check result show normalcy, The recording medium which recorded the program for considering it as a means to perform predetermined error handling, and making it function when a means to memorize the application from said supply center to the predetermined field of the IC card concerned, and said check result show an error and in which computer reading is possible.

[Detailed Description of the Invention]

[0001]

[Field of the Invention] This invention relates to the card system which memorizes the application supplied by the supply center which supplies application to the IC card published by the card issue center.

[0002]

[Description of the Prior Art] For example, the supplier (purveyor of service) of application supplies the application for cards at the IC card which the card publisher published to each user, and the card system which aims at multiple-purpose use of an IC card is known. In such a system, the user can receive the predetermined service by a purveyor of service by downloading desired application to a self IC card, and performing application built into the IC card, for example.

[0003]

[Problem to be solved by the invention] In the above card systems, supply of the application to the IC card by an inaccurate purveyor of service is prevented, for example, and the structure which can receive supply of application safely is needed.

[0004] Moreover, when performing attestation processing of the supplier (purveyor of service) of application from a viewpoint of holding the safety of a system and the attestation processing long-time [complication and]-izes, there is a possibility of reducing the response of a system.

[0005] Moreover, the proper fee collection management to each purveyor of service is wanted for the supply situation of the application to each IC card to be correctly grasped by the card publisher, for example, to realize etc. in the industry.

[0006] This invention was made in view of the situation mentioned above, and aims at offering the card system which can supply application safely. Moreover, this invention sets it as other purposes to offer the card system which can prevent complication and long time-ization of attestation processing of the supplier of application. Moreover, this invention sets it as other purposes to offer the system which can manage the registration situation of the application for cards to an IC card.

[0007]

[Means for solving problem] [the card system concerning the 1st viewpoint of this invention] in order

to attain the above-mentioned purpose Are the application supplied to the IC card published by the card issue center by the supply center the card system to memorize, and [said IC card] The permission table about the application with which supply was permitted by said card issue center is memorized. It is distinguished whether the application supplied from said supply center is registered into said permission table. When said application is registered into said permission table, this application is memorized to the predetermined field of the IC card concerned, and when said application is not registered into said permission table, predetermined error handling is performed.

[0008] When according to such composition the permission table about the application which the card issue center permitted beforehand is stored in the IC card and application is downloaded to an IC card, the justification of the application is checked with reference to a permission table. Since the justification can be checked within a card, without asking a card issue center the justification of application by this whenever it downloads, the card system in which safety is high and attestation in a short time is possible is realizable.

[0009] About each aforementioned application, it may be set to said permission table by the check information concerned by which application machine ****** derivation is carried out, respectively, and [said IC card] Answer supply of the application from said supply center, and check information is drawn based on said supplied application. When you may compare with the check information on the applicable application set as said permission table and said check information agrees When said supplied application may be memorized to the predetermined field of the IC card concerned and said check information does not agree, you may perform predetermined error handling.

[0010] Said check information may also contain a hash value.

[0011] The signature by a management organization may be given to said permission table. Thereby, since it is checking the permission from both a card issue center and a management organization with consent substantially, checking application using a permission table can increase the safety of a system further. Moreover, the dishonest act by an application supplier's (purveyor of service) cooperation etc. can be prevented card issue origin by giving the signature by a disinterested management organization, for example.

[0012] [moreover, the IC card concerning the 2nd viewpoint of this invention] It is the IC card for card systems which memorizes the application supplied to the IC card published by the card issue center by the supply center. The permission table about the application with which supply was permitted by said card issue center is memorized. It is distinguished whether the application supplied from said supply center is registered into said permission table. When said application is registered into said permission table, this application is memorized to the predetermined field of the IC card concerned, and when said application is not registered into said permission table, it is characterized by what predetermined error handling is performed for.

[0013] [moreover, the card system concerning the 3rd viewpoint of this invention] Are the application supplied to the IC card published by the card issue center by the supply center the card system to memorize, and [said supply center] Acquire attestation information from said card issue center, supply said attestation information and application which were acquired to said IC card, and [said IC card] When the justification of said attestation information from said supply center is checked and a check result shows normalcy, the application from said supply center is memorized to the predetermined field of the IC card concerned, and when a check result shows an error, it is characterized by what predetermined error handling is performed for.

[0014] According to such composition, when supplying application to an IC card, the attestation information published by the card issue center is needed. Registration of the application to the IC card by the service offer server which does not acquire attestation information from a card issue center can be eliminated by this, and a safe card system can be offered.

[0015] When said supply center supplies application to an IC card, A card identification signal is acquired from the IC card of the supply place of application. May supply said card identification signal and application identification signal which were acquired to said card issue center, and [said card issue center] [the information about the application based on said application identification signal] Said supply center may be supplied by making into said attestation information what was enciphered with the key of the IC card specified by said card identification signal, and said IC card may check the justification of said attestation information using the key of the IC card concerned.

[0016] Moreover, when a supply center supplies application to an IC card, May acquire a random number from the IC card of the supply place of application, may supply the random number and application identification signal which were acquired to said card issue center, and [said card issue center] You may supply said supply center by making into said attestation information what enciphered the information about the application based on said random number and said application identification signal with the key of the card issue center concerned. Said IC card may check the justification of said attestation information which generated the random number, supplied said supply center, and was supplied from said supply center using the key of said card issue center.

[0017] Said IC card is followed on deletion of the application memorized by the IC card concerned. The deletion certificate about the application for deletion may be drawn up, the supply center of the supply origin of the application for [said] deletion may be supplied, and said supply center may transmit the deletion certificate from said IC card to said card issue center.

[0018] Since a supply center acquires attestation information from a card issue center by this whenever application is supplied to an IC card, the card issue center can grasp certainly that application was

supplied to each IC card. Moreover, when an IC card publishes the certificate about deletion of application to a supply center and a supply center submits the certificate to a card issue center, the card issue center can grasp certainly that application was deleted from each IC card. Moreover, about each IC card, since the card issue center can grasp registration and deletion of application certainly, it can perform proper fee collection management to a supply center.

[0019] [moreover, the IC card concerning the 4th viewpoint of this invention] Are the application supplied to the IC card published by the card issue center by the supply center the IC card for card systems to memorize, and [said IC card] The attestation information which said supply center acquired from said card issue center is received. When the justification of this attestation information is checked and a check result shows normalcy, the application from said supply center is memorized to the predetermined field of the IC card concerned, and when a check result shows an error, it is characterized by what predetermined error handling is performed for.

[0020] [moreover, the recording medium concerning the 5th viewpoint of this invention] It is the recording medium which recorded the program for making it function as an IC card which memorizes the application which is published by the card issue center and supplied by the supply center in a computer and in which computer reading is possible. A means to memorize the permission table about the application with which this computer was permitted to supply by said card issue center, A means to distinguish whether the application supplied from said supply center is registered into said permission table, When said application was registered into said permission table by said distinction means and it is distinguished, When said application was not registered into said permission table by means to memorize this application to the predetermined field of the IC card concerned, and said distinction means and it is distinguished, the program for considering it as a means to perform predetermined error handling, and making it function is recorded.

[0021] [moreover, the recording medium concerning the 6th viewpoint of this invention] It is the recording medium which recorded the program for making it function as an IC card which memorizes the application which is published by the card issue center and supplied by the supply center in a computer and in which computer reading is possible. A means to receive the attestation information to which said supply center acquired this computer from said card issue center, When a means to check the justification of said attestation information, and said check result show normalcy, When a means to memorize the application from said supply center to the predetermined field of the IC card concerned, and said check result show an error, the program for considering it as a means to perform predetermined error handling, and making it function is recorded.

[0022]

[Mode for carrying out the invention] The card system concerning the form of operation of this invention is hereafter explained with reference to Drawings. This card system is for downloading and

building the various applications for cards supplied by the supplier (purveyor of service) of application into the IC card which the card publisher published to the user.

[0023] (The 1st embodiment) The system composition figure of the card system concerning the 1st embodiment of this invention is shown in drawing 1. This card system is equipped with the card issue center 1, the management center 2, the card processing terminal 3, IC card 4, and service offer server 5 of each purveyor of service so that it may be illustrated.

[0024] The card issue center 1 performs issue of IC card 3 to a user etc. In issue of this IC card 3, [the card issue center 1] Based on the application for cards which each service offer server 5 distributes, the predetermined table (permission table) about the application for cards is created, and grant of a signature is received from the management center 2 to the permission table. And the permission table on which the signature was given, and predetermined card information, including card ID etc., are recorded on IC card 3 for issue, and are published.

[0025] [the permission table generated by the card issue center 1] For example, as shown in drawing 2, information, including Application ID, a hash value, etc., is set up about the application for cards which each service offer server 5 offers for every purveyor-of-service ID for identifying the service offer server 5. This hash value is generated based on the information on a meaning, for example for every applications for cards, such as a program of the application for cards.

[0026] The management center 2 gives a signature (administrator signature) to the permission table which the card issue center 1 generated according to the demand from the card issue center 1.

[0027] The card processing terminal 3 is equipped with IC card reader / writer, and mainly performs data ****** between IC card 4 and the service offer server 5 etc. For example, the card processing terminal 3 notifies the demand of download of the application for cards inputted by the user to IC card 4 through a card reader/writer. The card ID received from IC card 4 according to this is transmitted to the service offer server 5 with the download demand of the application for cards. Moreover, transmission etc. makes application for cards received from the service offer server 5 IC card 4 through a card reader/ writer.

[0028] IC card 4 is equipped with IC chip which has MPU, ROM, RAM, EEPROM, etc., and as this IC chip is shown, for example in drawing 3, it is equipped with the control part 41, the memory 42, and I/O control unit 43 which are realized when MPU executes the program memorized by ROM etc.

[0029] The control part 41 transmits the card ID memorized by the memory to the card processing terminal 3 according to the predetermined notice from the card processing terminal 3. And the control part 41 will create the hash value of the application for cards, if the downloaded application for cards is

received from the card processing terminal 3. And the application ID of the received application for cards and the created hash value are compared with the preset value of the permission table memorized by the memory 42.

[0030] When Application ID and the hash value which were compared are in agreement The control part 41 memorizes the application for cards received to the storage area for memorizing the application for cards in a memory 42 noting that the application for cards is beforehand permitted to the card issue center 1.

[0031] moreover, when Application ID and the hash value which were compared are not in agreement The control part 41 performs predetermined error handling, such as transmitting and carrying out the error display of the error signal to the card processing terminal 3, without distinguishing, if it is not the application for cards which the card issue center 1 permitted, and memorizing the application for cards to a predetermined storage area.

[0032] A memory 42 memorizes a permission table, card information, the application for cards (card ID etc.), etc. I/O control unit 43 controls data communications with the card processing terminal 3.

[0033] The service offer server 5 is a server for performing offer of the application for cards to IC card 4 etc. The service offer server 5 is read from the memory part which answers the download demand of the application for cards from the card processing terminal 3, and does not illustrate the applicable application for cards, and transmits to the card processing terminal 3 of a requiring agency.

[0034] Next, in the system concerning this 1st embodiment, the processing in the case of registering the application for cards into IC card 4 is explained with reference to drawing 4. For example, a certain user sets IC card 4 to the card processing terminal 3, and inputs the download demand of the application for cards (application ID:123) which the service offer server 5 (purveyor-of-service ID:BBB) offers. According to this, the card processing terminal 3 notifies the input of a demand of download to IC card 4, acquires Card ID etc., and transmits to the service offer server 5 with the download demand of the application for cards of Application ID "123" (Step S1, S2).

[0035] The service offer server 5 which received the download demand reads the application for cards of the applicable application ID "123", and transmits to IC card 4 through the card processing terminal 3 (Step S3).

[0036] IC card 4 generates a hash value (for example, "23") about the received application for cards (Step S4). And it is distinguished [the application ID of the received application for cards "123", and] whether the generated hash value "23" agrees with the preset value of the purveyor's of service ID "BBB" permission table memorized by the memory 42 (Step S5).

[0037] When Application ID and the hash value which were compared agree, noting that IC card 4 is just application to which the received application for cards is permitted from the card issue center 1 It stores in the field for applications of a memory 42 for cards (Step S6).

[0038] moreover, when Application ID and the hash value which were compared do not agree with the preset value of a permission table for example [the IC card / the received application for cards] noting that IC card 4 is unjust application which has not obtained the permission from the card issue center 1 For example, it eliminates without memorizing the application for cards to the storage area for the applications for cards, and predetermined error handling of transmitting an error signal to the card processing terminal 3 is performed (Step S7).

[0039] Thus, the permission table about the application for cards which the card issue center 1 permitted beforehand to IC card 4 is stored. When downloading the application for cards to IC card 4, the justification of the application for cards is checked with reference to a permission table. Since the justification can be checked within a card, without asking the card issue center 1 the justification of the application for cards by this whenever it downloads, the card system in which safety is high and attestation in a short time is possible is realizable.

[0040] moreover, [the permission table stored in IC card 4] Since the signature as an administrator by the management center 2 is given, it is consent to check application for cards using this permission table as substantially as checking the permission from both the card issue center 1 and the management center 2. Therefore, the safety of a system can be increased further. Moreover, the dishonest act by a purveyor's of service cooperation etc. can be prevented card issue origin by giving the signature by the disinterested management center 2, for example.

[0041] Moreover, it is good also as system composition except the management center 2. In this case, like the above-mentioned explanation, although the signature by the management center 2 is not given to a permission table at a third party, since the check based on a permission table is performed within IC card 4, the card system in which safety is high and attestation in a short time is possible is realizable.

[0042] Moreover, when the case where the application for cards which each purveyor of service offers is added, and a new purveyor of service are added, you may make it the card issue center 1 supply a new permission table to IC card 4 through the card processing terminal 3.

[0043] Moreover, the data for a check memorized on a permission table is not limited to a hash value. For example, you may use the arbitrary functions which can derive a meaning numerical value, data, etc. to each application for cards.

[0044] Moreover, application for cards of a purveyor of service may be stored in a memory part, and service offer equipment equipped with a card reader writer may be used. In this case, a user sets IC card 4 in service offer equipment, and inputs the write-in demand to IC card 4 of the desired application for cards. According to this input, service offer equipment reads the specified application for cards from a memory part, and passes it to IC card 4. IC card 4 checks application for cards based on a permission table, like the above-mentioned explanation, when the justification is checked, it records it on the predetermined storage area of a memory 42, and when it distinguishes that it is unjust, it performs error handling of eliminating the received application.

[0045] (The 2nd embodiment) The system composition figure of the card system concerning the 2nd embodiment of this invention is shown in drawing 5. This card system is equipped with the card issue center 6, the card processing terminal 7, IC card 8, and service offer server 9 of each purveyor of service so that it may be illustrated.

[0046] The card issue center 6 performs issue of IC card 8 to a user etc. The card issue center 6 records the encryption key (secret key for cards) of a meaning on the memory of each IC card 8 for issue for every card. Moreover, the card issue center 6 memorizes the key table which matches Card ID and the encryption key (public key for cards) of each IC card 8 as shown, for example in drawing 6. Moreover, the card issue center 6 memorizes the table on which the hash value generated about the application for cards which each service offer server 9 offers based on Application ID and its application for cards is matched.

[0047] The card issue center 6 will read the hash value corresponding to the application ID contained in key demand information, if the key demand information which contains Application ID, for example with Card ID and the purveyor of service ID is received from the service offer server 9. And the encryption key (public key for cards) corresponding to the card ID contained in key demand information is read from a key table, the hash value previously acquired with the encryption key is enciphered, the signature by the card issue center 6 is given to the enciphered hash value, and it transmits to the service offer server 9 of a requiring agency.

[0048] Moreover, the card issue center 6 generates and memorizes fee collection information including the time of purveyor-of-service ID and Card ID as shown in drawing 7, Application ID, and a registration date etc. based on the key demand information received from the service offer server 9. And it charges to the purveyor of service who supplies the application for cards to IC card 8 based on this fee collection information. The method of fee collection is arbitrary, for example, whenever the record time to a card carries out predetermined time progress, you may make it the predetermined amount of money charged for every application at application offer origin.

[0049] Moreover, [the card issue center 6 / server / 9 / service offer] if the certificate about deletion of

the purveyor of service ID and application is received With reference to fee collection information, the fee collection information applicable to receiving data is specified, and information, including the deletion time of application etc., is set up as opposed to the fee collection information. In addition, this certificate is information published by IC card 8 to the service offer server 9, when the application for cards is deleted from IC card 8, for example, it contains Application ID, Card ID, etc. which were deleted. As for this certificate, the signature may be made, for example with the secret key of IC card 8. In this case, the card issue center 6 checks the justification of a certificate by checking a signature using the public key of IC card 8.

[0050] The card processing terminal 7 is equipped with IC card reader / writer, and mainly performs data ****** between IC card 8 and the service offer server 9 etc. For example, the card processing terminal 7 notifies download of the application for cards or a demand of deletion inputted by the user to IC card 8 through a card reader/writer. The card ID received from IC card 8 according to this is transmitted to the service offer server 9 with the download demand of the application for cards, or the notice of a deletion demand. Moreover, the card processing terminal 7 transmits a hash value, application for cards, etc. which were received from the service offer server 9 and which were enciphered [which were enciphered and were access-demanded] to IC card 4 through a card reader/ writer.

[0051] IC card 8 is equipped with IC chip which has MPU, ROM, RAM, EEPROM, etc., and as this IC chip is shown, for example in drawing 8, it is equipped with the control part 81, the memory 82, and I/O control unit 83 which are realized when MPU executes the program memorized by ROM etc.

[0052] The control part 81 transmits the card ID memorized by the memory to the card processing terminal 7 according to the notice of the demand of the download from the card processing terminal 7, the demand of deletion of the application for cards, etc. having been inputted.

[0053] Moreover, the control part 81 will verify the signature given to the enciphered hash value, if a hash value, application for cards, etc. which were enciphered as the access demand (write-in demand) to IC card 8 from the service offer server 9 are received through the card processing terminal 7. And if a signature is right, the enciphered hash value will be decrypted using the encryption key (secret key for cards) memorized by the memory 82. Next, it compares with the hash value which created the decrypted hash value based on the received application for cards. And when the compared hash value is in agreement, the control part 81 memorizes the application for cards received to the storage area for memorizing the application for cards in a memory 82. Moreover, when the compared hash value is not in agreement, the control part 81 performs predetermined error handling, such as transmitting and carrying out the error display of the error signal to the card processing terminal 7, without memorizing the application for cards to a predetermined storage area.

[0054] Moreover, the control part 81 will delete the specified application for cards from a memory 82, if

the deletion demand of the application for cards from the service offer server 9 etc. is received through the card processing terminal 7. And the certificate containing the application ID of the eliminated application for cards, the card ID of the IC card 8, etc. is transmitted to the service offer server 9 through the card processing terminal 7. In addition, you may give the signature which used the secret key of IC card 8 for this certificate.

[0055] A memory 82 memorizes an encryption key (secret key for cards), a card publisher's public key, card information, the application for cards (card ID etc.), etc. I/O control unit 83 controls data communications with the card processing terminal 7.

[0056] The service offer server 9 is a server for performing offer of the application for cards to IC card 8 etc. The service offer server 9 answers the download demand of the application for cards from the card processing terminal 7. For example, the card ID received with the download demand, the application ID of the demanded application for cards, and key demand information including the purveyor of service ID are generated, it transmits to the card issue center 6, and the enciphered hash value is received from the card issue center 6. And the service offer server 9 is read from the memory part which does not illustrate the application for cards applicable to a download demand, and transmits to IC card 8 through the card processing terminal 7 with the enciphered hash value and a predetermined access demand (write-in demand).

[0057] Moreover, the service offer server 9 answers the notice of a deletion demand of the application for cards from the card processing terminal 7, and transmits the deletion demand of the specified application to IC card 8 through the card processing terminal 7. And the certificate from IC card 8 is received through the card processing terminal 7, and this certificate is transmitted to the card issue center 6.

[0058] Next, in the system concerning this 2nd embodiment, the processing in the case of registering the application for cards into IC card 8 is explained with reference to drawing 9. For example, a certain user sets IC card 8 (card ID:3232) to the card processing terminal 7, and inputs the download demand of the application for cards which the service offer server 9 offers. According to this, the card processing terminal 7 notifies the input of a demand of download to IC card 8. Card ID "3232" etc. is acquired and it transmits to the service offer server 9 with the download demand (the application ID for download is included) of the application for cards (Step S11, S12).

[0059] The service offer server 9 which received the download demand generates the received card ID "3232", the application ID of the demanded application for cards, and key demand information including the purveyor of service ID, and transmits to the card issue center 6 (Step S13).

[0060] The card issue center 6 answers reception of key demand information, and reads the hash value

corresponding to the application ID contained in this receiving data. Moreover, the encryption key "1212" corresponding to Card ID "3232" is read from a key table, and a hash value is enciphered with the encryption key, and the signature which used the secret key of the card issue center 6 for the enciphered hash value is given, and it transmits to the service offer server 9 of a requiring agency (Step S14). Moreover, the card issue center 6 generates and memorizes fee collection information using the receiving data from the service offer server 9 (Step S15). And based on fee collection information, a purveyor of service charges Card ID "3232" to offering the application for cards.

[0061] Moreover, the service offer server 9 transmits the application for cards required as the enciphered hash value which received from the card issue center 6, and an access demand (write-in demand) to IC card 8 through the card processing terminal 7 (Step S16).

[0062] IC card 8 is verified about the signature given to the enciphered hash value which received using the public key of a card issue center. If a signature is right, the hash value enciphered using the encryption key (secret key for cards) will be decrypted. And it is distinguished whether it agrees with the hash value which the decrypted hash value created based on the received application for cards (Step S17).

[0063] When the compared hash value agrees, IC card 8 stores the received application for cards in the field for applications of a memory 82 for cards noting that it checked the justification of the transmitting agency (Step S18).

[0064] moreover, when the compared hash value does not agree, or when a signature is unjust IC card 8 is eliminated, for example, without memorizing the application for cards to the storage area for the applications for cards, and predetermined error handling of transmitting an error signal to the card processing terminal 7 is performed (Step S19).

[0065] Next, in the system concerning this 2nd embodiment, the processing in the case of deleting the application for cards from IC card 8 is explained with reference to drawing 10. For example, a user sets IC card 8 (card ID:3232) to the card processing terminal 7, and inputs the deletion demand of the application for cards memorized by IC card 8. According to this, the card processing terminal 7 notifies the input of deletion of application of a demand to IC card 8. Card ID "3232" etc. is acquired and it transmits to the service offer server 9 with the notice of a deletion demand of the application for cards (the application ID for deletion is included) (Step S21, S22).

[0066] The service offer server 9 which received the deletion demand transmits the access demand (deletion demand) for deleting the specified application for cards to IC card 8 through the card processing terminal 7 (Step S23). While deleting the application for cards with which IC card 8 was specified according to this from a memory 82, the certificate in which having deleted this application for

cards is shown is drawn up (Step S24, S25). And the drawn-up certificate is transmitted to the service offer server 9 through the card processing terminal 7 (Step S26).

[0067] The service offer server 9 transmits the certificate received from IC card 8 to the card issue center 6 (Step S27). The card issue center 6 checks that the application for cards has been deleted from the received certificate, and sets the deletion time of the application for cards etc. as applicable fee collection information (Step S28).

[0068] Thus, when registering the application for cards into IC card 8, that to which the card issue center 6 signed what enciphered the information on the application for cards with the key peculiar to IC card 8 is needed. Thereby, since the information for attestation which is not effective is generated by only the card with the card issue center 6, registration of the application for cards to IC card 8 by the inaccurate service offer server 9 can be eliminated, and a safe card system can be offered. Moreover, by making the certificate about deletion of the application for cards publish by IC card 8, and submitting the certificate to the service offer server 9 etc. In the card issue center 6, since registration and deletion can be certainly grasped to the application for cards to each IC card 8, proper fee collection management can be performed.

[0069] Moreover, also when deleting the application for cards of IC card 8, you may make it need attestation by the card issue center 6 like the case of registration. In this case, the service offer server 9 acquires the hash value and signature which were enciphered from the card issue center 6 like the case of registration, and transmits a code key to IC card 8 with the deletion demand of the application for cards.

[0070] Moreover, application for cards of a purveyor of service may be stored in a memory part, and service offer equipment equipped with a card reader writer may be used. In this case, a user sets IC card 8 in service offer equipment, and inputs the write-in demand to IC card 8 of the desired application for cards. According to this input, service offer equipment transmits Card ID and Application ID to the card issue center 6, acquires the hash value and signature to this which were enciphered from the card issue center 6, and passes them to IC card 8 with the specified application for cards. Like the above-mentioned explanation, a signature and the check of a hash value are performed, IC card 8 records the application for cards on the predetermined storage area of a memory 82, when the justification is checked, and when it distinguishes that it is unjust, it performs error handling of eliminating the received application.

[0071] Moreover, in the card issue center 6, what is enciphered with the encryption key of IC card 8 is not limited to the hash value corresponding to Application ID, but should just be information [meaning / the application for cards]. For example, a signature is given to what enciphered Application ID with the encryption key of IC card 8, and you may make it supply the service offer server 9. In this case, after IC card 8 verifies a signature, it decrypts the enciphered application ID with an encryption key, and distinguishes whether it is the application ID of the received application for cards.

[0072] Moreover, in advance of the registration to IC card 8 of the application for cards, IC card 8 generates a random number, and you may make it include the random number in the object of the signature by the card issue center 6. As shown in drawing 11 in this case, the service offer server 9 requires generation of a random number from IC card 8 (Step S31). According to this, IC card 8 transmits the random number which generated and generated the random number to the service offer server 9 (Step S32). The service offer server 9 transmits the application ID of the received random number and the application for cards for download etc. to the card issue center 6 (Step S33).

[0073] According to this, the card issue center 6 reads the hash value corresponding to the received application ID. And the permission information which enciphered the read hash value and the received random number with the secret key of the card issue center 6 is generated, and fee collection of as opposed to [again (Step S34)] a purveyor of service in the card issue center 6 which transmits to the service offer server 9 of a requiring agency is performed. The service offer server 9 transmits the application for cards required as the permission information received from the card issue center 6 to IC card 8 with an access demand (Step S35).

[0074] IC card 8 decrypts the received permission information with the public key of the card issue center 6, and acquires a hash value and a random number. And the acquired random number is compared with the random number which self generated. Moreover, IC card 8 compares the created hash value which was created based on the received application for cards with the hash value which received (Step S36).

[0075] and when the both sides of the collation result of a random number and the collation result of a hash value are normal When the received application for cards is stored in the predetermined field of a memory 82 (Step S37) and one of collation results shows an error It eliminates without memorizing the application for cards to a predetermined field, and predetermined error handling of transmitting an error signal to the card processing terminal 7 is performed (Step S38).

[0076] Thus, since it restricts once and the effective information for attestation is created by using a random number, the level of security can be raised. Moreover, also in this example, the object of the encryption in the card issue center 6 is not limited to the hash value corresponding to Application ID, but should just be information [meaning / that application for cards]. For example, you may make it supply the service offer server 9 by making into permission information what enciphered a random number and Application ID with the secret key in the card issue center 6. In this case, IC card 8 performs the collation about a random number and the collation about Application ID which were decrypted and obtained.

[0077] Moreover, the code method used in the above-mentioned work example is not limited to a secret

key cryptosystem, but may use a common key encryption system.

[0078] Moreover, the card processing terminals 3 and 7 in the form of the 1st and the 2nd operation contain a personal digital assistant (cellular-phone machine) etc.

[0079] In addition, the system of this invention cannot be based on a system for exclusive use, but can be realized using the usual computer systems. For example, by installing this program from the media (a floppy disk, CD-ROM, etc.) which stored the program for performing above-mentioned operation in the computer The card issue centers 1 and 6 which perform above-mentioned processing, the management center 2, the card processing terminal 2, and 7 grades can be constituted. In addition, when OS is realized by cooperation of an assignment or OS, and application, you may store an above-mentioned function only through portions other than OS.

[0080] In addition, it is also possible to superimpose a program on a carrier wave and to distribute through a communication network. For example, this program may be put up for the bulletin board (BBS) of a communication network, and this may be distributed through a network. And above-mentioned processing can be performed by starting this program and performing like other application programs under control of OS.

[0081]

[Effect of the Invention] As explained above, according to this invention, supply of the application to the IC card by the supply center which has not received attestation by a card issue center is eliminated, and supply of safe application is enabled.

[Brief Description of the Drawings]

[Drawing 1] It is the system composition figure of the card system concerning the 1st embodiment of this invention.

[Drawing 2] It is a figure for explaining a permission table.

[Drawing 3] It is a figure for explaining the composition of the IC card used by the card system of drawing 1.

[Drawing 4] It is a figure for explaining the processing in the case of registering the application for cards into an IC card in the card system of drawing 1.

[Drawing 5] It is the system composition figure of the card system concerning the 2nd embodiment of this invention.

[Drawing 6] It is a figure for explaining a key table.

[Drawing 7] It is a figure for explaining fee collection information.

[Drawing 8] It is a figure for explaining the composition of the IC card used by the card system of drawing 5.

[Drawing 9] It is a figure for explaining the processing in the case of registering the application for cards into an IC card in the card system of drawing 5.

[Drawing 10] It is a figure for explaining the processing in the case of deleting the application for cards from an IC card in the card system of drawing 5.

[Drawing 11] It is a figure for explaining other examples of processing in the case of registering the application for cards into an IC card in the card system of drawing 5.

[Explanations of letters or numerals] 1, 6 Card issue center 2 Management centers 3 and 7 Card processing terminals 4 and 8 IC cards 5 and 9 Service offer servers 41 and 81 Control parts 42 and 82 Memories 43 and 83 I/O control unit

[Translation done.]